Anti-Spam Updates

Activity Coordination Meeting
March 2006
Kevin Hill

Connie/spelling

Anti-Spam Updates

- Black listed by anti-spam sites
- Greylisting - Next Generation Spam Fighting

Working with Anti-Spam Companies

Blacklisted (Backscatter)

- Spam Cop started blacklisting the email gateways on 2/14/06.
  - We ask for assistance. No response was given on why we were blacklisted
  - A few sites had us blacklisted for "back-scatter"
    - What we are doing is RFC compliant but that doesn't always help!

Blacklisted (Back-scatter)

- Back-scatter
  - Backscatter occurs when an email system accepts a message for delivery and then the system determines that the message can not be delivered and sends an undeliverable mail notification.
- What to do?
  - Users should request that fnal.gov be added to the white list at remote site.
  - CD changed email system to prevent back-scatter (enabled 2/21)
- Still blacklisted!

Blacklisted (Relay)

- Is FNAL a Spam Relay?
- Incoming email marked as spam delivered to 'user'@fnal.gov
  - 'user'@fnal.gov forwards email offsite.
  - 'user'@fnal.gov forwards email to 'user'@'machine'.fnal.gov then forwards email offsite.
- Email marked as spam sent offsite
  - Some mail systems treat us as spam relays

Blacklisted (Relay)

- Make recommendation
- Solution options;
  - Don't allow offsite forwards (~4k active)
  - Follow AV policy; Delete obvious spam
    - Set threshold score for delete, anything below that will be treated as it is now.
  - Enable spam filter on outgoing email. Delete obvious spam
  - Quarantine server review
    - Most complicated to implement. Requires time and hardware.
- May need more systems!

Greylisting

What It Does

- Requires all email from unknown servers to retry sending their message a short time later.

- Virus infected computers spewing spam (and viruses) won't retry. (yet).

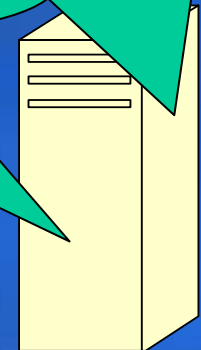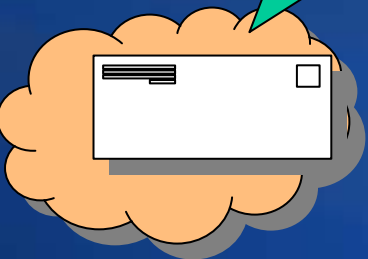- Many system administrators report up to 90% spam reduction.

How Messages Go

Who uses it

- Query HEP labs…
- University of Bergen - the Norwegian university of Bergen is using greylisting on their mail server.

- Texas A&M University - This Texas university is using greylisting: www.tamu.edu/network-services/smtp-relay/greylisting.html

- Leibniz Rechen Zentrum - LRZ is a major German internet hub for academic institutions in southern Germany. They started using greylisting as a method of limiting spam a couple of months ago: www.lrz-muenchen.de/aktuell/ali2052/

- APNIC (Asia Pacific Network Information Centre) - This organisation, one of the five major internet registries of the world, is also using greylisting: www.apnic.net/info/contact/greylisting.html

- RWTH - RWTH is a large German University. They have a page on their greylisting (german) here: www.rz.rwth-aachen.de/infodienste/email/greylisting.php

How It Works

- Records a triplet consisting of *remote server ip address*, *envelope sender*, and *envelope recipient*.

- If that triplet hasn't been seen before, enter it in the database and reject the message with a temporary failure code.

- If the triplet has been seen more than 5 minutes before, and less than the expire time for entries, accept the message.

Possible Fallout

- Some people will see a delay getting email from someone new. This will be between 5 minutes and however long the remote server takes to retry delivery. Generally not more than 1 hour.

- A few sites won't retry. They are broken, but need to be dealt with.

Solutions

- WhiteLists
  - Our greylist package provides downloadable whitelists of known broken/good email servers.
  - Local whitelists are maintainable.
- Opt-Out
  - We can maintain an 'opt-out' list, for people who prefer to get more spam.

Rollout Timeline

- Upgrade Hepa machines version of Postfix and install local mysql server. *1 day (Done)*
- Install sqlgrey Greylisting service. Configure postfix to warn only (in the mail logs) to prebuild databases. *15-30 days (Done)*
- Monitor Logs for legit mail that isn't getting through. *Ongoing*
- Turn greylisting on "for real". *(3/8/2006)*